Trattamento dei dati personali in conformità con il Regolamento Europeo 2016/679 (GDPR) : linee guida per i professionisti

Attività pratiche, valutazione del rischio e misure di sicurezza

02/10/2018

Ing. Francesca Merighi

Coordinatrice area tematica
Sicurezza delle Informazioni e Protezione dei Dati Personali
dell' Ordine degli Ingegneri di Bologna

ORDINE INGEGNERI BOLOGNA

Commissione dell'Informazione
Area Tematica Sicurezza delle Informazioni e Protezione dei Dati Personali

In collaborazione con gli Ordine degli Ingegneri di Ancona, Ferrara, Forlì-Cesena, Ravenna, Reggio Emilia, Rimini

Il vademecum per il professionista

1. **Identifica i trattamenti** di dati personali svolti nell'attività lavorativa come titolare o come responsabile del trattamento
2. **Raccogli le informazioni** utili sui trattamenti
3. **Valuta l'adeguatezza delle misure di sicurezza** in funzione del rischio sui trattamenti
4. **Adotta misure di sicurezza aggiuntive** se necessario abbassare il livello di rischio
5. Se il rischio è alto, esegui una **valutazione d'impatto**
6. **Redigi il registro** delle attività di trattamento, come titolare e/o come responsabile
7. **Designa eventuali responsabili del trattamento**
8. **Redigi e distribuisci le informative** sul trattamento
9. **Raccogli i consensi** al trattamento (quando necessario)
10. **Organizza la gestione dei dati personali** per essere pronto a soddisfare i diritti degli interessati in tempi congrui
11. **Gestisci le eventuali violazioni** di dati personali

[1] Identificare i trattamenti di dati personali
Cosa sono i dati personali e i trattamenti

Trattamento di **dati personali**

Qualsiasi operazione o insieme di operazioni applicate a dati personali o insiemi di dati personali (es. raccolta, la conservazione, modifica, l'estrazione, la consultazione, l'uso, la comunicazione o divulgazione, la distruzione, ecc.)

Qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»)

- NO persone giuridiche o aziende
- NO persone in alcun modo identificabili (es. numero di condomini in un condominio)

Durante le attività lavorative svolgo operazioni su dati relativi a persone fisiche?

SI → Ogni operazione effettuata sui dati personali è o fa parte di un trattamento

NO → Le mie attività lavorative non rientrano nell'ambito di applicazione del GDPR

[1] Identificare i trattamenti di dati personali
Titolare o responsabile del trattamento?

TITOLARE

la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali

I titolare distribuisce le informative e raccoglie i consensi degli interessati

RESPONSABILE

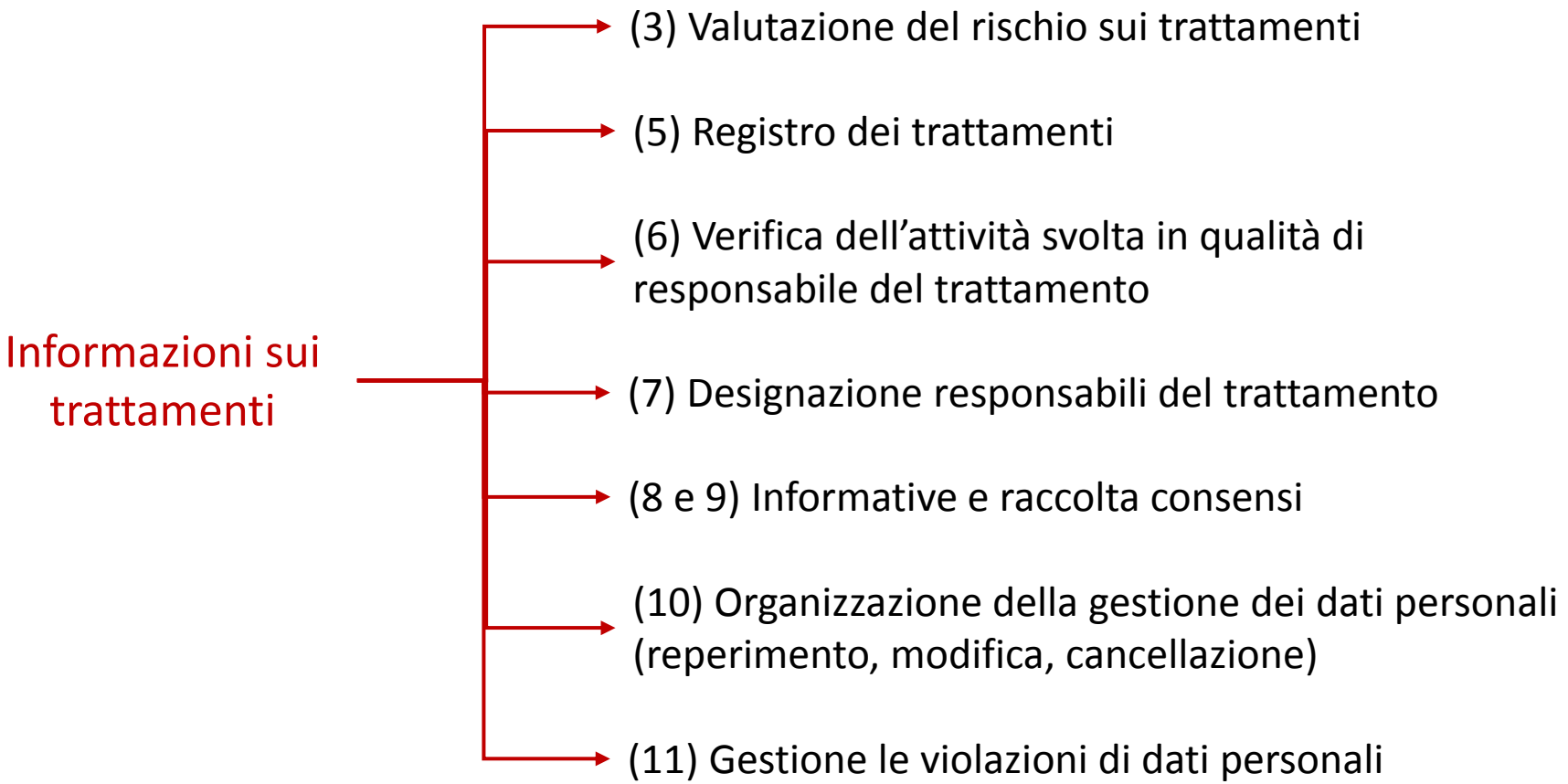
la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento

Il responsabile è istruito dal titolare sulle modalità di trattamento dei dati

Il vademecum per il professionista

1. **Identifica i trattamenti** di dati personali svolti nell'attività lavorativa come titolare o come responsabile del trattamento
2. **Raccogli le informazioni** utili sui trattamenti
3. **Valuta l'adeguatezza delle misure di sicurezza** in funzione del rischio sui trattamenti
4. **Adotta misure di sicurezza aggiuntive** se necessario abbassare il livello di rischio
5. Se il rischio è ancora alto, esegui una **valutazione d'impatto**
6. **Redigi il registro** delle attività di trattamento, come titolare e/o come responsabile
7. **Designa eventuali responsabili del trattamento**
8. **Redigi e distribuisci le informative** sul trattamento
9. **Raccogli i consensi** al trattamento (quando necessario)
10. **Organizza la gestione dei dati personali** per essere pronto a soddisfare i diritti degli interessati in tempi congrui
11. **Gestisci le eventuali violazioni** di dati personali

[2] Raccogliere informazioni utili sui trattamenti



[3] Valutazione del rischio sui trattamenti
I rischi in generale

Che cos'è il *rischio*?

E' la potenzialità che una **minaccia** si concretizzi in un **evento indesiderato**.

Lo ***scenario di rischio*** include la descrizione di

- ***minaccia***
  - è propria di una ***sorgente di rischio***
    - la sorgente di rischio ha capacità di portare avanti la minaccia ***capacità sorgente di rischio***
  - può concretizzarsi solo se
    - il sistema target ha almeno un difetto che può essere sfruttato ***vulnerabilità***
- ***evento indesiderato***
  - ha delle conseguenze di una certa ***gravità***

maggiore è la capacità delle sorgenti di rischio e la vulnerabilità del sistema target tanto maggiore è la ***probabilità*** che la minaccia si concretizzi

Il rischio è tanto più alto quanto è **grave l'evento indesiderato** e **probabile che la minaccia si concretizzi**

Il vademecum per il professionista

1. **Identifica i trattamenti** di dati personali svolti nell'attività lavorativa come titolare o come responsabile del trattamento
2. **Raccogli le informazioni** utili sui trattamenti
3. **Valuta l'adeguatezza delle misure di sicurezza** in funzione del rischio sui trattamenti
4. **Adotta misure di sicurezza aggiuntive** se necessario abbassare il livello di rischio
5. Se il rischio è ancora alto, esegui una **valutazione d'impatto**
6. **Redigi il registro** delle attività di trattamento, come titolare e/o come responsabile
7. **Designa eventuali responsabili del trattamento**
8. **Redigi e distribuisci le informative** sul trattamento
9. **Raccogli i consensi** al trattamento (quando necessario)
10. **Organizza la gestione dei dati personali** per essere pronto a soddisfare i diritti degli interessati in tempi congrui
11. **Gestisci le eventuali violazioni** di dati personali

[3] Valutazione del rischio sui trattamenti
Esempio di scenario di rischio generico

La casa di una persona risaputamente ricca ha una finestre aperte

- *Evento indesiderato*: furto
- ***Gravità dell'evento***: la casa contiene molti degli averi del proprietario -> **MASSIMA**
- *Minaccia*: un ladro si introduce in casa attraverso la finestra aperta
- *Sorgente di rischio*: ladro
- *Capacità della sorgente di rischio*: (la minaccia attira ladri anche con alte capacità «professionali» in quanto il bottino del furto appare appetibile) -> MASSIMA
- *Vulnerabilità*: (la finestra è aperta) -> MASSIMA
- ***Probabilità della minaccia***: (massima capacità delle sorgenti di rischio e massima vulnerabilità) -> **MASSIMA**
- **Livello di rischio:** (Gravità massima, Probabilità massima) **-> MASSIMO**

[3] Valutazione del rischio sui trattamenti
I rischi sui trattamenti: la gravità

- Devono essere devono essere considerati solo i rischi relativi al trattamento dei dati personali che hanno **impatto sugli interessati,** la gravità del rischio è identificata in base alle conseguenze dell'evento indesiderato sull'interessato
- La ***gravità*** del rischio viene definita in base alle categorie di dati personali relativi al trattamento. Dipende da
- effetti che ha l'evento indesiderato sull'interessato (***effetti pregiudizievoli***)
- in alcuni casi da quanto è identificabile l'interessato dai dati trattati (***identificabilità***)

Evento indesiderato sui dati personali	Calcolo gravità
divulgazione o all'accesso non autorizzato	identificabilità + effetti pregiudizievoli sull'interessato
modifica non autorizzata ai dati o al trattamento oppure mancanza di disponibilità dei dati o del trattamento (perdita, distruzione, ecc.	effetti pregiudizievoli sull'interessato

[3] Valutazione del rischio sui trattamenti
I rischi sui trattamenti: la probabilità

- La ***probabilità*** del rischio sui trattamenti è definita in base alla **capacità delle sorgenti di rischio** e le **vulnerabilità degli asset di supporto al trattamento**
- Se le categorie di interessati destano particolare interesse (es. gli interessati sono target appetibili) oppure vengono trattati dati su larga scala è probabile che la minaccia risulti appetibile per sorgenti di rischio con alte capacità.
- Gli ***asset di supporto*** sono i beni che vengono utilizzati durante il trattamento, es:
  - supporti cartacei
  - PC e server
  - reti
  - supporti removibili, ecc.

[3] Valutazione del rischio sui trattamenti
I rischi sui trattamenti: il livello di rischio accettabile

- Il **livello di rischio** può essere ***accettabile***, ovvero non è considerato indispensabile adottare ulteriori misure di sicurezza o eseguire analisi più approfondite (valutazione d'impatto) o altrimenti non accettabile.
- E' responsabilità del titolare/responsabile del trattamento definire il livello di rischio accettabile, non c'è una scala universalmente riconosciuta.

Il vademecum per il professionista

1. **Identifica i trattamenti** di dati personali svolti nell'attività lavorativa come titolare o come responsabile del trattamento
2. **Raccogli le informazioni** utili sui trattamenti
3. **Valuta l'adeguatezza delle misure di sicurezza** in funzione del rischio sui trattamenti
4. **Adotta misure di sicurezza aggiuntive** se necessario abbassare il livello di rischio
5. Se il rischio è ancora alto, esegui una **valutazione d'impatto**
6. **Redigi il registro** delle attività di trattamento, come titolare e/o come responsabile
7. **Designa eventuali responsabili del trattamento**
8. **Redigi e distribuisci le informative** sul trattamento
9. **Raccogli i consensi** al trattamento (quando necessario)
10. **Organizza la gestione dei dati personali** per essere pronto a soddisfare i diritti degli interessati in tempi congrui
11. **Gestisci le eventuali violazioni** di dati personali

[4] Adozione di ulteriori misure di sicurezza a riduzione del rischio

Ridurre il rischio significa ridurre o la gravità dell'evento indesiderato o la probabilità del concretizzarsi della minaccia

Riduzione della gravità

- Crittografia: trasformazione da rendere i dati illeggibili a meno della conoscenza di un segreto
- pseudonimizzazione: memorizzazione dei dati identificativi e i dati «sensibili» su supporti diversi e collegamento tra gli stessi attraverso uno pseudonimo
- minimizzazione dei dati: limitazione dei dati raccolti

Riduzione della probabilità

Misure di sicurezza a risoluzione delle vulnerabilità

- tecniche
- organizzative

Il vademecum per il professionista

1. **Identifica i trattamenti** di dati personali svolti nell'attività lavorativa come titolare o come responsabile del trattamento
2. **Raccogli le informazioni** utili sui trattamenti
3. **Valuta l'adeguatezza delle misure di sicurezza** in funzione del rischio sui trattamenti
4. **Adotta misure di sicurezza aggiuntive** se necessario abbassare il livello di rischio
5. Se il rischio è ancora alto, esegui una **valutazione d'impatto**
6. **Redigi il registro** delle attività di trattamento, come titolare e/o come responsabile
7. **Designa eventuali responsabili del trattamento**
8. **Redigi e distribuisci le informative** sul trattamento
9. **Raccogli i consensi** al trattamento (quando necessario)
10. **Organizza la gestione dei dati personali** per essere pronto a soddisfare i diritti degli interessati in tempi congrui
11. **Gestisci le eventuali violazioni** di dati personali

[5] Valutazione d'impatto

- Valutazione del rischio approfondita e secondo una precisa metodologia
- Necessaria solo se il trattamento rappresenta un rischio alto per le persone fisiche
- Richiede competenze e tempo
- Disponibile tool gratuiti
  - Tool del CNIL (autorità francese)
  - Tool delle PMI

Il vademecum per il professionista

1. **Identifica i trattamenti** di dati personali svolti nell'attività lavorativa come titolare o come responsabile del trattamento
2. **Raccogli le informazioni** utili sui trattamenti
3. **Valuta l'adeguatezza delle misure di sicurezza** in funzione del rischio sui trattamenti
4. **Adotta misure di sicurezza aggiuntive** se necessario abbassare il livello di rischio
5. Se il rischio è ancora alto, esegui una **valutazione d'impatto**
6. **Redigi il registro** delle attività di trattamento, come titolare e/o come responsabile
7. **Designa eventuali responsabili del trattamento**
8. **Redigi e distribuisci le informative** sul trattamento
9. **Raccogli i consensi** al trattamento (quando necessario)
10. **Organizza la gestione dei dati personali** per essere pronto a soddisfare i diritti degli interessati in tempi congrui
11. **Gestisci le eventuali violazioni** di dati personali

[6] Registro dei trattamenti in qualità di titolare e/o responsabile

- Riassume le attività di trattamento
- Prima documentazione da esibire in caso di ispezione del Garante della Privacy
- Deve essere congruente con le informative e le designazioni dei responsabili del trattamento
- Contiene anche la descrizione delle misure di sicurezza
- Consigliato allegare anche la valutazione del rischio che dimostra l'adeguatezza delle misure adottate

Il vademecum per il professionista

1. **Identifica i trattamenti** di dati personali svolti nell'attività lavorativa come titolare o come responsabile del trattamento
2. **Raccogli le informazioni** utili sui trattamenti
3. **Valuta l'adeguatezza delle misure di sicurezza** in funzione del rischio sui trattamenti
4. **Adotta misure di sicurezza aggiuntive** se necessario abbassare il livello di rischio
5. Se il rischio è ancora alto, esegui una **valutazione d'impatto**
6. **Redigi il registro** delle attività di trattamento, come titolare e/o come responsabile
7. **Designa eventuali responsabili del trattamento**
8. **Redigi e distribuisci le informative** sul trattamento
9. **Raccogli i consensi** al trattamento (quando necessario)
10. **Organizza la gestione dei dati personali** per essere pronto a soddisfare i diritti degli interessati in tempi congrui
11. **Gestisci le eventuali violazioni** di dati personali

[8 e 9] Gestione delle informative e dei consensi

- Le informative devono essere distribuite solo se ci si trattano i dati in qualità di titolare
- Le informative e le richieste di consenso devono essere espresse in termini semplici e comprensibili (principio di trasparenza)
- In caso di cambiamenti nei trattamenti occorre ridistribuire le informative
- E' utile indicare la versione e tenere storico sulle informative

Problemi aperti

- Come distribuire l'informativa?
- Come dimostrare di aver distribuito l'informativa?

Il vademecum per il professionista

1. **Identifica i trattamenti** di dati personali svolti nell'attività lavorativa come titolare o come responsabile del trattamento
2. **Raccogli le informazioni** utili sui trattamenti
3. **Valuta l'adeguatezza delle misure di sicurezza** in funzione del rischio sui trattamenti
4. **Adotta misure di sicurezza aggiuntive** se necessario abbassare il livello di rischio
5. Se il rischio è ancora alto, esegui una **valutazione d'impatto**
6. **Redigi il registro** delle attività di trattamento, come titolare e/o come responsabile
7. **Designa eventuali responsabili del trattamento**
8. **Redigi e distribuisci le informative** sul trattamento
9. **Raccogli i consensi** al trattamento (quando necessario)
10. **Organizza la gestione dei dati personali** per essere pronto a soddisfare i diritti degli interessati in tempi congrui
11. **Gestisci le eventuali violazioni** di dati personali

[10] Organizzazione della gestione dei dati personali

Soddisfare diritto all'accesso, oblio, rettifica in tempi congrui presenta problemi:

- reperire tutti i dati personali dell'interessato
- esibire i dati personali dell'interessato senza divulgare dati non pertinenti
- modificare i dati personali dell'interessato senza modificare informazioni non pertinenti
- cancellare/offuscare i dati personali dell'interessato senza danneggiare informazioni non pertinenti

Soluzione ORGANIZZAZIONE -> PRIVACY BY DESIGN

- organizzazione di archivi cartacei ed elettronici
- adozione di software di ricerca e indicizzazione per i dati non strutturati
- Adozione di software gestionali «GDPR ready»

Il vademecum per il professionista

1. **Identifica i trattamenti** di dati personali svolti nell'attività lavorativa come titolare o come responsabile del trattamento
2. **Raccogli le informazioni** utili sui trattamenti
3. **Valuta l'adeguatezza delle misure di sicurezza** in funzione del rischio sui trattamenti
4. **Adotta misure di sicurezza aggiuntive** se necessario abbassare il livello di rischio
5. Se il rischio è ancora alto, esegui una **valutazione d'impatto**
6. **Redigi il registro** delle attività di trattamento, come titolare e/o come responsabile
7. **Designa eventuali responsabili del trattamento**
8. **Redigi e distribuisci le informative** sul trattamento
9. **Raccogli i consensi** al trattamento (quando necessario)
10. **Organizza la gestione dei dati personali** per essere pronto a soddisfare i diritti degli interessati in tempi congrui
11. **Gestisci le eventuali violazioni** di dati personali

[11] Gestione delle violazioni dei dati personali

- Tutte le violazioni dei dati personali devono essere registrate dal titolare/responsabile
- Il responsabile notifica le violazioni al titolare
- Se la violazione rappresenta un alto rischio per i diritti e le libertà di persone fisiche allora la violazione deve essere segnalata al Garante della Privacy
- Al Garante della Privacy deve essere inviato un documento tramite PEC contenente le informazioni sulla violazione, in particolare quelle necessarie al garante per valutare il rischio sui diritti e la libertà delle persone fisiche
- In alcuni casi la violazione deve essere comunicata anche all'interessato